In the Claims

1. (ORIGINAL) A relay module for connection to a door latch in a secure area, comprising:

a micro-controller decrypting encrypted communications from a reader in an unsecured area and comparing the decrypted communications to an expected code; and

a relay coupled to said micro-controller switching power to actuate said door latch if the comparison of said decrypted communications and said expected code indicates a correct match.

2. (ORIGINAL) The relay module of claim 1, wherein said relay module and said door latch are a single module.

3. (ORIGINAL) The relay module of claim 1, wherein said micro-controller enables said relay if the comparison indicates a correct match.

4. (ORIGINAL) The relay module of claim 3, wherein if said relay is enabled, power runs through said door latch to unlock a door.

5. (ORIGINAL) The relay module of claim 1, further comprising at least one buffer coupled to said micro-controller for receiving said encrypted communications from said reader.

6. (ORIGINAL) The relay module of claim 5, wherein said at least one buffer protects said micro-controller from being damaged if a spike occurs in said communications between said reader and said relay module.

7. (ORIGINAL) The relay module of claim 5, wherein said at least one buffer rectifies any voltage level drop between said reader and said relay module.

8. (ORIGINAL) A method of switching a door latch in a secure area, said method comprising the steps of:

decrypting encrypted communications from a reader in an unsecured area and comparing the decrypted communications to an expected code; and

switching power to actuate said door latch if the comparison of said decrypted communications and said expected code indicates a correct match.

9. (ORIGINAL) The method of claim 8, wherein a micro-controller implements said decrypting and comparing steps.

10. (ORIGINAL) The method of claim 9, wherein a relay coupled to said micro-controller implements said switching step.

11. (ORIGINAL) The method of claim 10, wherein said relay module and said door latch are a single module.

12. (ORIGINAL) The method of claim 9, wherein said micro-controller enables said relay if the comparison indicates a correct match.

13. (ORIGINAL) The method of claim 12, wherein if said relay is enabled, power runs through said door latch to unlock a door.

14. (ORIGINAL) The method of claim 8, further comprising the step of receiving said encrypted communications from said reader.

15. (ORIGINAL) The method of claim 14, wherein at least one buffer coupled to said micro-controller implements said receiving step.

16. (ORIGINAL) The method of claim 15, wherein said at least one buffer protects said micro-controller from being damaged if a spike occurs in said communications between said reader and said relay module.

17. (ORIGINAL) The method of claim 15, wherein said at least one buffer rectifies any voltage level drop between said reader and said relay module.

18. (ORIGINAL) An access control system, comprising:

a reader located in an unsecured area for determining access rights in response to presentation of a card and generating encrypted communications;

a relay module located in a secure area for receiving said encrypted communications from said reader, decrypting said encrypted communications, and comparing the decrypted communications to an expected code;

a door latch coupled to said relay module, said door latch actuated by said relay module switching power if the comparison of said decrypted communications and said expected code indicates a correct match.

19. (ORIGINAL) The access control system according to claim 18, wherein said generated encrypted communications comprises an access command for said relay module.

20. (ORIGINAL) The access control system according to claim 18, wherein said door latch is directly connected to said relay module.

21. (ORIGINAL) The access control system according to claim 20, wherein said relay module and said door latch are a single module.

22. (ORIGINAL) The access control system according to claim 18, wherein said reader comprises logic functions and a database residing in said reader.

23. (ORIGINAL) The access control system according to claim 22, wherein said database holds information including access times, users, hot-listing, holidays, and the like.

24. (ORIGINAL) The access control system according to claim 22, wherein said reader is autonomous if communications are cut or a master computer is brought down.

25. (ORIGINAL) The access control system according to claim 18, wherein said reader is a smartcard reader and said card is a smartcard.

26. (ORIGINAL) The access control system according to claim 25, wherein said smartcard implements an anti-passback feature.

27. (ORIGINAL) The access control system according to claim 18, wherein said reader is a biometric reader.

28. (ORIGINAL) The access control system according to claim 18, wherein said relay. module is a storage relay module.

29. (ORIGINAL) The access control system according to claim 18, wherein said relay module comprises:

a micro-controller for decrypting encrypted communications from a reader in an unsecured area and for comparing the decrypted communications to an expected code; and

a relay coupled to said micro-controller for switching power to actuate said door latch if the comparison of said decrypted communications and said expected code indicates a correct match.

30. (ORIGINAL) The access control system according to claim 29, wherein said relay module further comprises at least one buffer coupled to said micro-controller for receiving said encrypted communications from said reader.

31. (ORIGINAL) The access control system according to claim 18, wherein said communications are encrypted using 128-bit AES, 3DES, DES, or skipjack.

32. (ORIGINAL) A method of controlling access to a secure area, said method comprising the steps of:

determining access rights using a reader located in an unsecured area in response to presentation of a card and generating encrypted communications;

receiving said encrypted communications from said reader using a relay module located in a secure area for, decrypting said encrypted communications, and comparing the decrypted communications to an expected code; and

actuating a door latch coupled to said relay module using said relay module by switching power if the comparison of said decrypted communications and said expected code indicates a correct match.

33. (ORIGINAL) The method according to claim 32, wherein said generated encrypted communications comprises an access command for said relay module.

34. (ORIGINAL) The method according to claim 32, wherein said door latch is directly connected to said relay module.

35. (ORIGINAL) The method according to claim 34, wherein said relay module and said door latch are a single module.

36. (ORIGINAL) The method according to claim 32, wherein said reader comprises logic functions and a database residing in said reader.

37. (ORIGINAL) The method according to claim 36, wherein said database holds information including access times, users, hot-listing, holidays, and the like.

38. (ORIGINAL) The method according to claim 36, wherein said reader is autonomous if communications are cut or a master computer is brought down.

39. (ORIGINAL) The method according to claim 32, wherein said reader is a smartcard reader and said card is a smartcard.

40. (ORIGINAL) The method according to claim 39, wherein said smartcard implements an anti-passback feature.

41. (ORIGINAL) The method according to claim 32, wherein said reader is a biometric reader,

42. (ORIGINAL) The method according to claim 32, wherein said relay module is a storage relay module.

43. (ORIGINAL) The method according to claim 32, wherein said relay module comprises:

a micro-controller for decrypting encrypted communications from a reader in an unsecured area and for comparing the decrypted communications to an expected code; and

a relay coupled to said micro-controller for switching power to actuate said door latch if the comparison of said decrypted communications and said expected code indicates a correct match.

44. (ORIGINAL) The method according to claim 43, wherein said relay module further comprises at least one buffer coupled to said micro-controller for receiving said encrypted communications from said reader.

45. (ORIGINAL) The method according to claim 32, wherein said communications are encrypted using 128-bit AES, 3DES, DES, or skipjack.

46. (ORIGINAL) A method of providing antipassback in an access control system, said method comprising the steps of

reading antipassback information from a read/write smartcard presented to a read/write reader;

checking permissions using said read/write reader; and

updating said read/write smartcard with updated antipassback information using said reader.

47. (ORIGINAL) A method of providing antipassback in an access control system, said method comprising the steps of:

reading antipassback information from a read/write smartcard presented to a read/write reader;

determining if said antipassback information passes an integrity check based on an entry/exit pattern; and

if the antipassback information passes the integrity check, writing updated antipassback information to said read/write smartcard and granting access.

48. (ORIGINAL) The method according to claim 47, further comprising the step of, if the antipassback information fails to satisfy the integrity check, denying access.

49. (CURRENTLY AMENDED) The method according to ~~any one of claims 46 to 48~~ claim 46, wherein said antipassback is able to be disabled.

50. (CURRENTLY AMENDED) The method according to ~~any one of claims 46 to 49~~ claim 46, wherein said antipassback is able to be normalized so that a cardholder may proceed through an antipassback area without violating antipassback rules.

51. (ORIGINAL) The method according to claim 50, wherein a database of readers is updated with an antipassback flag.